

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-302008

(43)Date of publication of application : 13.11.1998

(51)Int.Cl.

G06F 17/60

G06F 5/00

G06F 15/00

H04L 9/08

(21)Application number : 09-126357

(71)Applicant : MITSUBISHI CORP

(22)Date of filing : 30.04.1997

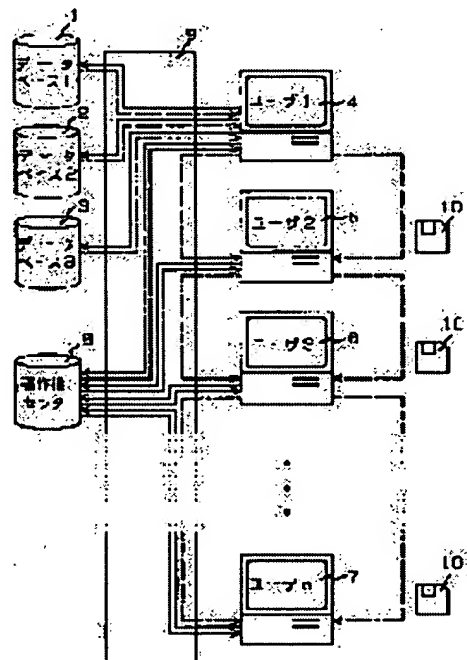
(72)Inventor : SAITO MAKOTO

(54) DATA CONTENTS DISTRIBUTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To distribute source data contents and work data contents by making a second user decode a ciphered scenario by using a secret key and reconstitute the work data contents based on a decoded work scenario.

SOLUTION: The second user who receives ciphered source data contents components along with a digitally signed work program pr sends the digitally signed work program to a copyright management center 8 and requests a second secret key for decoding the ciphered source data contents component. The copyright management center 8 transfers the second secret key to the second user in the case that a first user is the appropriate user of the source data contents for which the second secret key is requested. Then, the second user decodes the ciphered scenario by using the secret key and reconstitutes the work data contents based on the decoded work scenario.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-302008

(43) 公開日 平成10年(1998)11月13日

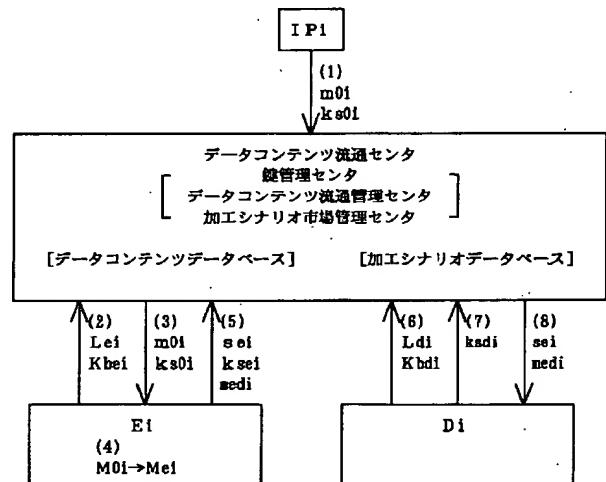
(51) Int.Cl. ⁸	識別記号	F I	
G 0 6 F 17/60		G 0 6 F 15/21	3 3 0
5/00		5/00	Z
15/00	3 3 0	15/00	3 3 0 Z
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
			6 0 1 E
審査請求 未請求 請求項の数 5 F D (全 20 頁) 最終頁に続く			
(21) 出願番号	特願平9-126357	(71) 出願人	000005979 三菱商事株式会社 東京都千代田区丸の内2丁目6番3号
(22) 出願日	平成9年(1997)4月30日	(72) 発明者	斉藤 誠 東京都千代田区丸の内2丁目6番3号 三 菱商事株式会社内
		(74) 代理人	弁理士 南條 眞一郎

(54) 【発明の名称】 データコンテンツ流通システム

(57) 【要約】

【発明の課題】 原データコンテンツ及び加工データコンテンツを流通させるためのシステムを提供する。

【解決手段】 データコンテンツとしてオブジェクトを取り扱い、データコンテンツの加工はオブジェクトであるデータコンテンツを加工プログラムによって加工することによって行われ、加工データコンテンツは原データコンテンツと加工プログラムによる加工内容を記載した加工シナリオとによって表現される。流通するのは暗号化された加工シナリオのみであり、暗号化加工シナリオを入手したユーザは鍵管理センタから入手した暗号鍵を用いて暗号化加工シナリオを復号し、加工シナリオに従ってデータベースから原データコンテンツを入手し加工データコンテンツを再構成する。加工シナリオの販売を希望する者がいる場合には、競売を行い加工シナリオの使用権を販売する。



【特許請求の範囲】

【請求項1】 データベースに保存されている原データコンテンツ及び前記原データコンテンツを第1ユーザが加工した加工データコンテンツをネットワーク上で第2ユーザに販売するデータコンテンツ流通システムであって：前記データコンテンツ流通システムでは、前記原データコンテンツが、データオブジェクトで構成され；前記加工データコンテンツが、前記データオブジェクトと前記データオブジェクトの加工内容を記載した加工シナリオから構成され；前記データコンテンツ流通システムが、データコンテンツ流通センタとデータベースから構成され；前記データコンテンツ流通センタが、鍵管理センタ、データコンテンツ流通管理センタ及び加工シナリオ流通管理センタから構成され；前記鍵管理センタが、秘密鍵生成、秘密鍵保管及び秘密鍵配送を行い；前記データコンテンツ流通管理センタが、前記データベースに保存されているデータコンテンツの広告及び販売を行い；前記加工シナリオ流通管理センタが、前記加工シナリオの広告及び販売を行い；前記第1ユーザが、前記データベースに保存されている原データコンテンツを利用して加工データコンテンツを作成し、該加工データコンテンツの加工シナリオを秘密鍵で暗号化して前記データベースに預託するとともに該秘密鍵を前記鍵管理センタに預託し；該暗号化加工シナリオ及び該秘密鍵が該加工データコンテンツの利用を希望する第2ユーザに配送され；該第2ユーザが該秘密鍵を用いて該暗号化加工シナリオ復号し、該復号された加工シナリオに基づいて該加工データコンテンツを再構成するデータコンテンツ流通システム。

【請求項2】 前記データベースが、データコンテンツを保存するデータコンテンツデータベースと加工シナリオを保存する加工シナリオデータベースから構成されている請求項1のデータコンテンツ流通システム。

【請求項3】 該原データコンテンツが該暗号化加工シナリオ及び該秘密鍵とともに第2ユーザに配送される請求項1のデータコンテンツ流通システム。

【請求項4】 データベースに保存されている前記原データコンテンツをデータコンテンツ加工者が加工した加工シナリオをネットワーク上でデータコンテンツ販売者に競売により売却するデータコンテンツ流通システムであって：前記データコンテンツ流通システムでは、前記原データコンテンツが、データオブジェクトで構成され；前記加工データコンテンツが、前記データオブジェクトと前記データオブジェクトの加工内容を記載した加工シナリオから構成され；前記データコンテンツ流通システムが、データコンテンツ流通センタとデータベースから構成され；前記データコンテンツ流通センタが、鍵管理センタ、データコンテンツ流通管理センタ及び加工シナリオ流通管理センタから構成され；前記鍵管理センタが、秘密鍵生成、秘密鍵保管及び秘密鍵配送を行

い；前記データコンテンツ流通管理センタが、前記データベースに保存されている前記データコンテンツの広告及び販売を行い；前記加工シナリオ流通管理センタが、前記加工シナリオの広告及び競売を行い；前記データコンテンツ加工者が、前記データベースに保存されている原データコンテンツを利用して加工データコンテンツを作成し、該加工データコンテンツの加工シナリオを前記データコンテンツ加工者の秘密鍵で暗号化して前記データベースに預託するとともに該秘密鍵を前記鍵管理センタに預託し；該加工シナリオの販売を希望する加工シナリオ販売者に競売を行い；該加工シナリオ販売者が該加工シナリオ用の秘密鍵を鍵管理センタに転送し；前記加工シナリオ流通管理センタが該加工シナリオ用の秘密鍵を前記データコンテンツ加工者の秘密鍵から該加工シナリオ販売者の秘密鍵に変更するデータコンテンツ流通システム。

【請求項5】 前記データベースが、データコンテンツを保存するデータコンテンツデータベースと加工シナリオを保存する加工シナリオデータベースから構成されている請求項4のデータコンテンツ流通システム。

【発明の詳細な説明】

【0001】

【技術分野】本発明は著作権デジタルデータコンテンツの流通、即ち、原デジタルデータコンテンツ及び加工されたデジタルデータコンテンツの流通における著作権管理システムに係るものである。

【0002】

【従来技術】アナログデータコンテンツは保存、複写、加工、転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルデータコンテンツは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルデータコンテンツの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0003】データコンテンツの利用法は単にその内容を参照するだけでなく、通常は得たデータコンテンツを保存、複写、加工することによってユーザが有効活用し、ユーザが加工したデータコンテンツを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオフラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータコンテンツとして登録することさえ可能であり、その場合にはデータコンテンツを加工したユーザも新たな情報提供者になることができる。

【0004】このような状況において、データベース化されたデータコンテンツの著作権をどのように取扱うか

が大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写、加工、転送等の2次利用について完成された著作権管理手段はない。本発明者らは特開平6-46419号(GB2269302A)及び特開平6-1410004号(USP5504933)で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平6-132916号(GB2272822A)でそのための装置を提案した。

【0005】また、特開平7-271865・EP677949A2(US08/416037)において、これらの上記先願発明をさらに発展させることによって、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータコンテンツの表示(音声化を含む)、保存等の1次利用及び複写、加工、転送等の2次利用における著作権管理方法を提案した。

【0006】この先願のデータベース著作権管理システムでは、著作権の管理を行うために、申し込まれた利用形態に対応した利用許可鍵の他に、著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を用い、暗号化して転送されたデータコンテンツを復号して、視聴・加工の利用を行い、保存・複写・転送の利用を行う場合にデータコンテンツは再暗号化される。

【0007】著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムはデータコンテンツの復号化/暗号化を行うとともに申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0008】また、本発明者らは具体的なデータベース著作権管理システムを特開平8-185448・EP704785A2(US08/536747)において提案した。このシステムは、データベース著作権管理システムを、暗号鍵を管理する鍵管理センタ及びデータベース著作権を管理する著作権管理センタから構成し、データベースから配布されるデータコンテンツは全て第1の暗号鍵によって暗号化(encrypt)され、データベースから直接にデータを利用する第1ユーザは、鍵管理センタに対して第1ユーザの情報を提示して利用形態に対応する鍵の要求を行い、第1ユーザから1次利用申込を受けた鍵管理センタは第1ユーザの情報を著作権管理センタに転送し、第1ユーザの情報を受け取った著作権管理センタはこの情報とともに著作権管理プログラムを鍵管理センタに転送し、著作権管理プログラムを受け取った鍵管理センタは著作権管理プログラムと利用形態に対応する第1の暗号鍵(crypt key)、第2の暗号鍵を第1ユーザに対して通信ネットワークを経由して転送し、第1の暗号鍵を受け取った第1ユーザは受け取った第1の暗号鍵を用いてデータを復号(decrypt)して利用し、以後デ

ータの保存、コピーあるいは転送を行う場合には第2の暗号鍵を用いて暗号化及び復号化が行われる。

【0009】データコンテンツが保存されずに外部記憶媒体にコピーされたときあるいは転送されたときには第1暗号鍵及び第2暗号鍵は廃棄され、第1ユーザが再度データコンテンツを利用する場合には著作権管理センタから第1暗号鍵と第2暗号鍵の再交付を受け、この第2暗号鍵の再交付を受けたことにより、第2ユーザへのデータコンテンツのコピーあるいは転送が行われたことが確認され、このことが著作権管理センタに記録される。

【0010】第2ユーザは著作権管理センタへの2次利用申込のときに第1ユーザの情報及び原著作権についての情報を著作権管理センタに提示する。著作権管理センタは利用形態に対応する許可鍵とともに暗号化された第2暗号鍵(視聴許可鍵)及び第3暗号鍵(利用形態に対応した許可鍵)及び著作権管理プログラムを第2ユーザに送信する。

【0011】一方、企業内等の組織においてコンピュータを相互に接続してLAN(Local Area Network)を構成することが広く行われているが、複数のネットワークを相互に接続し、複数のネットワーク全体をあたかも1つのネットワークであるかのように利用するインターネット(Internet)が世界的な規模で構成されている。

【0012】企業内等の組織内のLANには組織外に知られてはならない秘密情報が保管されていることが多い。そのため、そのような秘密情報は特定のユーザのみが利用できるようにする必要があり、外部への秘密情報の漏洩を防止するために、一般的にはアクセスコントロールが行われる。アクセスコントロール方法には、大きく分けてアクセス許可によって行う方法と、暗号化によって行う方法の2種類の方法がある。

【0013】アクセス許可によるアクセスコントロール方法は、USP5173939, 5220604, 5224163, 5315657, 5414772, 5438508, EP506435, JP開62-169540に述べられている。暗号化によるアクセスコントロール方法は、USP4736422, 5224163, 5400403, 5457746, 5584023, EP438154, 506435, JP開5-145923に述べられており、暗号化とデジタル署名によるアクセスコントロール方法が、USP4919545, 5465299に述べられている。

【0014】また、複数のLANをインターネットを経由して接続しあたかも単一のLANであるかのように利用するイントラネット(Intranet)が普及しつつある。このイントラネットにおいては本質的に窃取等に対する安全性を有しないインターネットを経由して情報交換を行うため、秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。伝送時の情報窃取を暗号化により防止することが、USP5504818, 551

5441に述べられており、その場合に複数の暗号鍵を用いることがUSP5504816, 5353351, 5475757及び5381480に述べられており、再暗号化を行うことがUSP5479514に述べられている。

【0015】暗号化する場合には、暗号鍵の受け渡しを含む暗号鍵管理が重要な問題となるが、暗号鍵生成をICカードによって行うことがUSP5577121に、暗号化／復号化をICカードによって行うことがUSP5347581, 5504817に各々述べられている。また、電子透かし技術がEP649074に述べられている。

【0016】ところで、コンピュータネットワークシステムの発展に伴い従来はスタンドアローンで使用されていた個々のコンピュータがネットワークシステムを介して接続され、データを共有するデータベースシステムが普及し、データだけでなくアプリケーションプログラム、さらにはオペレーティングシステムと呼ばれる基本ソフトウェアまでもネットワークを介して共有する分散オブジェクトシステムも提案されている。

【0017】分散オブジェクトシステムは、データコンテンツもソフトウェアもともにプログラムとデータからなるオブジェクトとして、サーバから供給される。分散オブジェクトシステムには、オペレーティングシステム、アプリケーションプログラム及びデータコンテンツはサーバが提供し、データコンテンツ処理及びデータコンテンツ保存は通常のコンピュータであるユーザ端末装置で行うオブジェクトコンテナと呼ばれるシステムと、オペレーティングシステム、アプリケーションプログラム及びデータはサーバが提供し、データ処理はネットワークコンピュータと呼ばれるユーザ端末装置が行うがデータコンテンツの保存はサーバが行うシステムがある。このシステムはさらに押し進めて、データコンテンツ処理もサーバが行い、ユーザ端末装置は入出力の機能のみしか有せず、システム全体が一つのコンピュータとして機能するものまでが考えられている。

【0018】一方、データヘッダとデータボディから構成される通常の形式のファイルの代わりに、データコンテンツとデータコンテンツを扱うプログラムとが一体化された「オブジェクト」を用いて種々の処理を行う「オブジェクト指向プログラミング(object oriented programming)」がある。オブジェクトはインスタンス(instance)と呼ばれる容器(envelope)中のスロット(slot)と呼ばれる格納箇所にインスタンス変数(instance variable)と呼ばれるデータが格納され、スロットの周囲は参照(referring)用、加工(processing)用、結合(binding)用等の1個又は複数のメソッド(method)と呼ばれる手続きで包囲されており、インスタンス変数を参照したり操作したりすることはメソッドを介してしか行うことはできず、この機能は隠蔽(encapsulation)と呼ばれる。ま

た、インスタンス変数の参照あるいは操作をメソッドに行わせる外部からの命令をメッセージと呼ぶ。

【0019】このことは見方を変えると、メソッドを介さなければ参照あるいは操作することができないインスタンス変数はメソッドによって保護されていることになる。このことを利用し、メソッドを暗号化し、暗号化されたメソッドを復号できるメッセージでなければインスタンス変数を参照あるいは操作することができないようにすることができる。この場合も通常のファイル形式を有するデータの場合と同様にメソッドの全てを暗号化してしまうとオブジェクトを利用することができなくなるため、メソッドの一部を暗号化しない。

【0020】また、ネットワークシステムの別の形態として、通信回線等のネットワーク基盤を提供する事業者が通信回線以外の課金システム、セキュリティシステム、著作権管理システム、認証システム等を提供し、サービス事業者がこれらのシステムサービスを利用してあたかも自己のシステムのようにしてネットワーク事業を行うライセンスネットワークと呼ばれる「賃貸ネットワークシステム」も構想されている。

【0021】先行技術の最後に本発明で利用する基本的な暗号関連技術について説明する。

【暗号鍵】秘密鍵(secret key)システムは暗号化と復号化が同じ鍵で行れるため「共通鍵システム」とも呼ばれ、鍵を秘密にしておく必要があることから「秘密鍵システム」と呼ばれる。秘密鍵を用いる暗号アルゴリズムとして代表的なものに米国標準局(National Bureau of Standards)のDES(Data Encryption Standard)システム、日本電信電話のFEAL(Fast Encryption Algorithm)システム、三菱電機のMISTYシステムがある。以下説明する実施例において秘密鍵を「Ks」と表示する。

【0022】これに対して公開鍵システムは、公開されている公開鍵(public key)とその鍵の所有者以外には秘密にされている専用鍵(private key)を用い、一方の鍵で暗号化し他方の鍵で復号化する暗号システムであり、代表的なものにRSA公開鍵システムがある。本明細書では公開鍵を「Kb」と、専用鍵を「Kv」と表示する。このときに、平文データコンテンツM(Material)を秘密鍵Ksを用いた暗号文Cmks(Cryptogram)に暗号化(Encryption)する操作を、

$Cmks = E(M, Ks)$

暗号文Cmksを暗号鍵Ksを用いて平文データコンテンツMに復号化(Decryption)する操作を、

$M = D(Cmks, Ks)$

また、平文データコンテンツMを公開鍵Kbを用いて暗号文Cmbkに暗号化する操作を、

$Cmbk = E(M, Kb)$

暗号文Cmbkを専用鍵Kvを用いて平文データコンテンツMに復号化する操作を、

$M = D(Cmkv, Kv)$

と、平文データコンテンツMを専用鍵Kvを用いて暗号文Cmkvに暗号化する操作を、

$Cmkv = E(M, Kv)$

暗号文Ckvを公開鍵Kbを用いて平文データコンテンツMに復号化する操作を、

$M = D(Cmkb, Kb)$

と表現する。

【0023】暗号技術はデータコンテンツの不正利用を不可能にするための手段であるが、その動作が完璧であるとの保証はないため、不正利用の可能性を完全に否定することができない。一方、電子透かし技術は不正利用を不可能にすることはできないが、不正利用が発見されたときには、電子透かしの内容を検証することにより不正利用であることを確定することができるが手段であり、種々の方法があるが日経エレクトロニクス683号、p.99～124に「電子透かし」がマルチメディア時代を守る（1997/2/24、日経BP社刊）に全般的に紹介されており、また同号、p.149～162、ウォルター ベンダー他「電子透かしを支えるデータ・ハイディング技術（上）」及び684号、p.155～168、「電子透かしを支えるデータ・ハイディング技術（下）」（IBM System Journal, vol.35, nos.3 & 4(International Business Machines Corporation)から転載）にも紹介されている。

【0024】

【発明の概要】本出願においては原データコンテンツ及び加工データコンテンツを流通させるためのシステムについて提案する。本出願において取り扱われるデータコンテンツはオブジェクトであり、データコンテンツの加工はオブジェクトであるデータコンテンツを加工プログラムによって加工することによって行われ、加工データコンテンツは原データコンテンツと加工プログラムによる加工内容を記載した加工シナリオとによって表現される。利用される原データコンテンツにはデータベースに保存されているものの他にデータ加工者が作成したものがあるが、データ加工者が作成したデータコンテンツもデータベースに保存することにより他のデータと同様に取り扱われる。流通するのは暗号化された加工シナリオのみであり、暗号化加工シナリオを入手したユーザは鍵管理センタから入手した暗号鍵を用いて暗号化加工シナリオを復号し、加工シナリオに従ってデータベースから原データコンテンツを入手し加工データコンテンツを再構成する。加工シナリオの販売を希望する者がいる場合には、競売により使用権を販売する。

【0025】

【実施例】図を参照しながら最適実施例を説明する。データコンテンツの加工は、原著作物データをアプリケーションプログラムである加工ツールを用いて編集することによって行われ、加工によって得られた加工データコ

ンテンツは、利用した原データコンテンツ、使用した加工ツールの情報及び加工内容データとによって表現することができる。すなわち、加工ツールを所有している場合には、原著作物データと加工内容データを入手することにより、加工著作物データを再現することが可能である。

【0026】初めに、デジタルデータの加工について説明する。デジタルデータの加工は加工用プログラム（加工ツール）を利用して原データコンテンツに改変を加えることによってなされるため、原データコンテンツ、加工ツール及び加工内容データ（加工シナリオ）が特定されることによって加工データコンテンツが再現される。いいかえれば、原データコンテンツ、加工ツールと加工シナリオが特定されなければ加工データコンテンツの再現は不可能である。

【0027】単一の原データコンテンツにより新しいデータコンテンツを作成する場合には、原データコンテンツAを改変して加工データコンテンツ「A'」を得る場合、原データコンテンツAにユーザがデータコンテンツXを付加することにより加工データコンテンツ「A+X」を得る場合、原データコンテンツAを原データコンテンツ要素A1, A2, A3・・・に分割し配列をA3, A2, A1のように変更して加工データコンテンツ「A''」を得る場合、原データコンテンツAを原データコンテンツ要素A1, A2, A3・・・に分割し第1ユーザのデータコンテンツXをX1, X2, X3・・・に分割しこれらを配列して加工データコンテンツ「A1+X1+A2+X2+A3+X3・・・」を得る場合等がある。これらの場合、原データの改変、原データコンテンツの配列変更、原データコンテンツとユーザデータコンテンツの組み合わせ、原データコンテンツの分割及びユーザデータコンテンツとの組み合わせ、が各々二次著作権の対象となり、これらの二次著作権を保護する必要がある。なお、ユーザが付加したデータコンテンツXにはユーザの著作権が存在することはいうまでもない。

【0028】複数の原データコンテンツを組み合わせることにより新しいデータコンテンツを作成する場合には、原データコンテンツA, B, C・・・を単純に組み合わせ加工データコンテンツ「A+B+C・・・」を得る場合、原データコンテンツA, B, C・・・にユーザがデータコンテンツXを付加することにより加工データコンテンツ「A+X」を得る場合、原データコンテンツA, B, C・・・を原データコンテンツ要素A1, A2, A3・・・, B1, B2, B3・・・, C1, C2, C3・・・に分割し組み合わせ配列を変更し加工データコンテンツ「A1+B1+C1+・・・+A2+B2+C2+・・・+A3+B3+C3+・・・」を得る場合、原データコンテンツA, B, C・・・を原データコンテンツ要素A1, A2, A3・・・, B1, B2, B3・・・, C1, C2, C3・・・に分割しユーザのデータコンテンツX1, X

2, $X3 \cdots$ を組み合わせて配列を変更して加工データコンテンツ「 $A1+B1+C1+X1+\cdots+A2+B2+C2+X2+\cdots+A3+B3+C3+X3+\cdots$ 」を得る場合等がある。これらの場合も、複数の原データコンテンツの組み合わせ、複数の原データコンテンツとユーザデータコンテンツの組み合わせ、複数の原データコンテンツの分割及び配列変更、分割された複数の原データコンテンツとユーザデータコンテンツの組み合わせ、が各々 2 次的著作権の対象となり、これらの 2 次的著作権を保護する必要がある。また、ユーザが付加したデータコンテンツ $X1, X2, X3 \cdots$ にはユーザの著作権が存在することはいうまでもない。

【0029】図面を用いて実施例 1 を説明する。図 1 に示されたのは、ユーザが 1 つの原著作物データを加工して、次のユーザに転送するデータ著作権管理システムの構成図である。この実施例において、1, 2, 3 はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、音声データあるいは映像データが暗号化されずに格納されたデータベースであり、9 は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供する CATV 回線等の通信回線、10 はフレキシブルディスク等の記録媒体、4 は第 1 ユーザ端末装置、5 は第 2 ユーザ端末装置、6 は第 3 ユーザ端末装置、7 は n 次ユーザ端末装置である。また、8 はデータ著作権を管理する著作権管理センタである。

【0030】これらのうちデータベース 1, 2, 3、著作権管理センタ 8、第 1 ユーザ端末装置 4、第 2 ユーザ端末装置 5、第 3 ユーザ端末装置 6 及び n 次ユーザ端末装置 7 は通信回線 9 に接続されている。この図において、破線で示された経路は暗号化されたデータコンテンツが伝送される経路であり、実線で示された経路は各ユーザ端末装置 4, 5, 6, 7 から各データベース 1, 2, 3 及び著作権管理センタ 8 への要求が伝送される経路であり、1 点鎖線で示された経路は各データベース 1, 2, 3 及び著作権管理センタ 8 から各ユーザ端末装置 4, 5, 6, 7 へ利用形態に対応する許可鍵、著作権管理プログラム及び暗号鍵が送信される経路である。

【0031】本実施例 1 においては、第 1 ユーザが用意する第 1 公開鍵 $Kb1$ 、第 1 公開鍵 $Kb1$ に対応する第 1 専用鍵 $Kv1$ 、第 2 公開鍵 $Kb2$ 、第 2 公開鍵 $Kb2$ に対応する第 2 専用鍵 $Kv2$ 、データベースが用意する第 1 秘密鍵 $Ks1$ 、第 2 秘密鍵 $Ks2$ が使用される。データベースでは、データコンテンツ M を第 1 秘密鍵 $Ks1$ を用いて暗号化し、

$$Cmks1 = E(M, Ks1)$$

第 1 秘密鍵 $Ks1$ を第 1 公開鍵 $Kb1$ を用いて暗号化する

$$Cks1kb1 = E(Ks1, Kb1)$$

とともに第 2 秘密鍵 $Ks2$ を第 2 公開鍵 $Kb2$ を用いて暗号化し、

$$Cks2kb2 = E(Ks2, Kb2)$$

これらの暗号化データコンテンツ $Cmks1$ 、暗号化第 1 秘密鍵 $Cks1kb1$ 及び暗号化第 2 秘密鍵 $Cks2kb2$ を第 1 ユーザに送信する。

【0032】第 1 ユーザ側では、暗号化第 1 秘密鍵 $Cks1kb1$ を第 1 専用鍵 $Kv1$ を用いて復号し、

$$Ks1 = D(Kv1, Cks1kb1)$$

復号された第 1 秘密鍵 $Ks1$ を用いて暗号化データコンテンツ $Cmks1$ を復号して

$$M = D(Ks1, Cmks1)$$

利用するとともに、暗号化第 2 秘密鍵 $Cks2kb2$ を第 2 専用鍵 $Kv2$ を用いて復号し、

$$Ks2 = D(Kv2, Cks2kb2)$$

復号された第 2 秘密鍵 $Ks2$ は以降におけるデータコンテンツの保存・複写・転送時の暗号/復号鍵として使用される。

【0033】第 1 ユーザが入手したデータコンテンツをそのまま複写して第 2 ユーザに供給した場合にはそのデータコンテンツに何等の変更も加えられていないため、そのデータコンテンツに第 1 ユーザの著作権は発生しない。しかし、第 1 ユーザが入手したデータコンテンツを基に新しいデータコンテンツを作成した場合あるいは他のデータコンテンツと組み合わせる等の手段を用いて新しいデータコンテンツを作成した場合にはその新しいデータコンテンツについて第 1 ユーザの 2 次著作権が発生し、この第 1 ユーザはその 2 次著作物の著作権者になる。同様に、第 2 ユーザが第 1 ユーザから入手したデータコンテンツを基に新しいデータコンテンツを作成した場合あるいは他のデータコンテンツと組み合わせる等の手段を用いてさらに新しいデータを作成した場合には、同様にその新しいデータコンテンツについて第 2 ユーザの 2 次著作権が発生し、この第 2 ユーザはその 2 次著作物の著作権者になる。

【0034】各データベース 1, 2, 3 にはテキストデータコンテンツ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータコンテンツ、デジタル音声データコンテンツ、デジタル映像データコンテンツが格納されており、第 1 ユーザ端末装置 4 からの要求に対してデータコンテンツ読み出し時に暗号化された状態で通信回線 9 を経由して第 1 ユーザ端末装置 4 に供給される。

【0035】データベースから入手するデータ著作権の管理は先願である特願平 6-237673 (特開平 8-185448, US 08/536747, EP 704785A2) に記載されている方法あるいは本件出願と同時に提出する出願に記載されている方法で行われる。

【0036】図 2 に示されたように、第 1 ユーザは単一のデータベースからあるいは複数のデータベースから入手した複数の原データコンテンツ $M1, M2, M3$ からデータコンテンツを構成するパーツ $M4, M5, M6$ を抽出

し、これらのパーツM4、M5、M6を利用して新しいデータコンテンツM7を生成する。

【0037】このように生成された新しいデータコンテンツM7を第1ユーザは第2ユーザ5に供給するが、新しいデータコンテンツM7には第1ユーザが原データコンテンツM1、M2、M3を加工することによって発生した2次的著作権の他に、データコンテンツM7を生成するための原料であるパーツM4、M5、M6を得た原データコンテンツM1、M2、M3についての原著作権も存在している。

【0038】これらの各原データコンテンツM1、M2、M3は表示以外の利用すなわち保存、加工、複写あるいは転送が行われるときには各データコンテンツとともに供給された各第2秘密鍵Ks21、Ks22、Ks23で暗号化されるが、

Cm1ks21=E (M1, Ks21)

Cm2ks22=E (M2, Ks22)

Cm3ks23=E (M3, Ks23)

各々の原データコンテンツの部品M4、M5、M6も同様に表示以外の利用が行われるときには各原データコンテンツとともに供給された第2秘密鍵Ks21、Ks22、Ks23で暗号化される。

Cm4ks21=E (M4, Ks21)

Cm5ks22=E (M5, Ks22)

Cm6ks23=E (M6, Ks23)

【0039】データ加工者である第1ユーザ4は加工プログラムPeに第1専用鍵Kv1を用いてデジタル署名を行い、

Spe=D (Pe, Kv1)

デジタル署名された加工プログラムPeとともに暗号化原データ部品Cm4ks21、Cm5ks22、Cm6ks23を通信回線9を経由してあるいは記録媒体10に記録して第2ユーザ5に供給する。

【0040】デジタル署名された加工プログラムPeとともに暗号化原データコンテンツ部品Cm4ks21、Cm5ks22、Cm6ks23を受け取った第2ユーザは、著作権管理センタ8に対してデジタル署名が行われた加工プログラムPeを提示して暗号化原データコンテンツ部品Cm4ks21、Cm5ks22、Cm6ks23を復号するための第2秘密鍵Ks21、Ks22、Ks23を要求する。

【0041】著作権管理センタ8は、第1公開鍵Kb1を用いて提示された加工プログラムのデジタル署名から第1ユーザ4を確認し、

Pe=E (Spe, Kb1)

その第1ユーザが第2秘密鍵Ks21、Ks22、Ks23を要求された原データコンテンツの正当な利用者であることを確認し、その第1ユーザが正当な利用者である場合には第2秘密鍵Ks21、Ks22、Ks23を第2ユーザに転送する。しかし、その第1ユーザが正当な利用者でない場合には第2秘密鍵Ks21、Ks22、Ks23を第2ユーザに転

送しない。

【0042】著作権管理センタに提示されたデジタル署名Speは第1ユーザが2次の著作権者であることを証明する正式な手続きとして著作権管理センタに登録される。

【0043】このデータの加工は原データコンテンツをその原データコンテンツに対応する加工プログラムを使用して加工することもできるが、原データコンテンツをオブジェクト指向ソフトウェアとして取り扱うようにすれば、より容易な加工とよりよいデータ著作権管理を行うことができる。また、さらに進んでエージェント指向ソフトウェアを採用すれば、ユーザは労することなくデータコンテンツの合成を行うことができる。

【0044】エージェント指向ソフトウェアは、自律性・適応性・協調性を兼ね備えたプログラムであり、従来のソフトウェアのようにすべての作業手順を具体的に指示しなくても、ユーザの一般的な指示のみに基づいてその自律性・適応性・協調性との特質により、ユーザの要求に応えることができる。このエージェントプログラムをデータ著作権管理システムの基本的なシステムの中に組み込み、ユーザのデータベース利用形態を監視させ、ユーザ端末装置に装備されたメタリング機能を利用して利用データ明細、課金情報などを含む情報をデータベース側あるいは著作権管理センタ側で収集するように構成することにより、ユーザのデータベース利用傾向をデータベース側あるいは著作権管理センタ側が知ることができ、よりきめの細かい著作権管理を行うことができる。したがって、エージェントプログラム及びデータも著作権保護の対象となり、原データコンテンツと同様に暗号化される。

【0045】著作権データはプログラムとデータコンテンツが一体化した「オブジェクト」としてコンピュータプログラミングあるいは各種処理において部品的な取り扱いをすることができる。

【0046】図3により実施例2を説明する。この実施例においては第1秘密鍵Ks1、第2秘密鍵Ks2、第3秘密鍵Ks3、平文である原著作権ラベルLc0及び平文である著作権管理プログラムPcが用いられる。図3に示されたデータ著作権管理システムは、データベース11、鍵管理センタ12、ユーザ13、13、13・・・およびこれらを相互に接続する通信回線14から構成されている。また、データベース11には情報提供者(Information Provider: IP)15、15、15・・・からデータコンテンツが供給されるが、場合によってはデータベース11を経由することなく情報提供者16、16、16・・・から通信回線14を経由して直接にユーザ13に対してデータコンテンツが供給されることがある。なお、本発明において利用されるデータコンテンツはプログラムとデータが組み合わされたオブジェクトである。また、データベース11には情報提供者15、1

5, 15・・・から第1ユーザ13にデータコンテンツが供給されるが、場合によっては情報提供者16, 16, 16・・・からネットワーク14を経由してあるいはCDROM等の情報記録媒体17を介してデータベース11を経由することなく直接に第1ユーザ13に対してデータコンテンツが供給されることもある。なお、この図において実線で示されたのは平文データ及び暗号鍵要求の経路、破線で示されたのは暗号化データコンテンツの経路、1点鎖線で示されたのは暗号鍵の経路である。第1ユーザ13は単なる利用者ではなく入手した複数の原データコンテンツを組み合わせたり、修正したりすることにより新しい著作物（2次著作物）を提供する情報提供者15あるいは16となりうる。

【0047】このデータ著作権管理システムにおいて、各情報提供者15, 16から提供される原データコンテンツは著作権を保護するために暗号化されている。したがって、第1ユーザ13が入手した暗号化原データコンテンツを利用するには暗号化原データコンテンツを復号化しなければならない。このシステムにおいてはそのための暗号鍵はすべて鍵管理センタ12に預けられ、鍵管理センタ12が管理する。なお、各情報提供者15, 16が採用する暗号方式は自由であるが、後で述べる2次利用以降で使用する暗号方式は鍵管理センタ12が採用する方式に限られる。

【0048】このシステムにおいて、平文である原データコンテンツM0は第1秘密鍵Ks1を用いて暗号化され、

$$Cm0ks1 = E(M0, Ks1)$$

原著作権ラベルLc0とともに情報提供者15からデータベース11を介してネットワーク14を経由して、情報提供者16から通信回線14を経由してあるいはCDROM等の情報記録媒体17を介して第1ユーザ13に供給される。

【0049】第1ユーザ13に供給される暗号化原データコンテンツCm0ks1には平文の原著作権ラベルLc0が付けられており、平文の原著作権ラベルLc0は1次利用鍵の入手等に利用される。すなわち、暗号化原データコンテンツCm0ks1は平文原著作権ラベルLc0と暗号化原データコンテンツCm0ks1から構成されている。平文原著作権ラベルLc0には原データコンテンツの原著者名、タイトル名、制作日等の一般情報の他に、使用しているアプリケーション・プログラム名、概要説明、使用料金及び課金方法等が記載されており、さらに必要に応じて暗号鍵の番号が記載されている。なお、平文原著作権ラベルLc0に原著作権者によるデジタル署名を付しておけば虚偽の申告を防止することができる。

【0050】供給された暗号化原データコンテンツCm0ks1の利用を希望する第1ユーザ13は、ネットワーク14を経由して鍵管理センタ12に原著作権ラベルLc0を提示して1次利用鍵K1の配布を要求する。

【0051】提示された原著作権ラベルLc0により、配布すべき秘密鍵が第1秘密鍵Ks1であることを確認した鍵管理センタ12は確認された第1秘密鍵Ks1をネットワークシステム14を経由して第1ユーザ13に配布する。配布された1次利用鍵K1を受信した時点で第1ユーザ13の装置は著作権管理モードになり、第1ユーザ13は1次著作権データコンテンツの利用が可能になる。一方、鍵管理センタ12は課金処理を行うとともに原データコンテンツの使用状況および第1ユーザ13のデータベース利用状況を把握する。

【0052】第1ユーザ13は配布された第1秘密鍵Ks1を用いて暗号化原データコンテンツCm0ks1を復号し、

$$M0 = D(Cm0ks1, Ks1)$$

利用する。復号された原データコンテンツM0が第1ユーザ13の装置内に保存される場合には第1秘密鍵Ks1を用いて再暗号化され、

$$Cm0ks1 = E(M0, Ks1)$$

再暗号化原データCm0ks1が保存される。再暗号化された原データコンテンツCm0ks1を再利用する場合には第1秘密鍵Ks1を用いて再復号化及び再暗号化が行われる。

【0053】原著作権データM0の加工を希望する第1ユーザ13はネットワーク14を経由して鍵管理センタ12に第2秘密鍵Ks2の配布を要求する。

【0054】第2秘密鍵Ks2の配布要求を受けた鍵管理センタ12は、ネットワーク14を経由して第2秘密鍵Ks2を第1ユーザ13に配布する。第2秘密鍵Ks2を受け取った第1ユーザ13は原データコンテンツM0の加工を行い、途中加工データM0'を得る。途中加工データコンテンツM0'がユーザ13の装置内に保存される場合には、第2秘密鍵Ks2によって暗号化される。

$$Cm0'ks2 = E(M0', Ks2)$$

加工が最終的に終了すると、第1ユーザ13は最終加工データコンテンツM1についてのデータ加工に関する2次著作権を行使するために第3秘密鍵Ks3を用意し、第3秘密鍵Ks3を鍵管理センタ12に登録する。なお、第3秘密鍵Ks3は第1ユーザ13ではなく鍵管理センタ12が用意し、第1ユーザ13からの要求により配布するようにしてもよい。

【0055】第1ユーザ13が加工データコンテンツM1を外部記憶媒体18への複製あるいはネットワーク14を介して転送する場合には、第3秘密鍵Ks3を用いて暗号化し、

$$Cm1ks3 = E(Ks3, M1)$$

第2ユーザ19へ供給する。

【0056】供給された暗号化加工データコンテンツCm1ks3の利用を希望する第2ユーザ19は、鍵管理センタ12に通信回線14を経由して第3秘密鍵Ks3の配布を要求する。第2ユーザ19からの第3秘密鍵Ks3の配

布要求を受けた鍵管理センタ12は、通信回線14を経由して第3秘密鍵Ks3を第2ユーザ19に配布する。第3秘密鍵Ks3を受け取った第2ユーザ19は、第3秘密鍵Ks3を用いて暗号化加工データコンテンツCm1ks3を復号化し、

$M1 = D(Ks3, Cm1ks3)$

利用する。その場合も、暗号化データコンテンツCm1ks3を再度利用する場合には第3秘密鍵Ks3を用いて復号化および暗号化が行われる。

【0057】[実施例3] ユーザが1つの原著作物データを加工して、次のユーザに転送する実施例3を図4により説明する。

【0058】この実施例において、データコンテンツの著作権を保護し、データ著作権を行使するために「ユーザラベル」、「著作権ラベル」及び「加工ラベル」が使用される。ユーザラベルにはラベル所有者の情報が記載されている。「著作権ラベル」には原著作物に関する情報が記載されている。「加工ラベル」には原著作権データに関する情報、加工ツールの情報及び加工データ（加工シナリオ）が記載されており、加工ツール情報の代わりに加工ツール（加工プログラム）を記載することもできる。

【0059】ユーザラベルはユーザがシステムに加入するときにユーザの情報に基づきデータ管理センタにより生成され、著作権ラベルは著作を行った著作者がデータ管理センタにその内容を提示することによりデータ管理センタによって生成され、加工ラベルはデータコンテンツの加工を行ったユーザがユーザラベルと加工シナリオをデータ管理センタに提示することによりデータ管理センタによって作成され、これらは各々のラベル所有者に転送されるとともに、データ管理センタ内に保存される。

【0060】(1) 原著作（データ所有者）Aは、著作権ラベルL0を提示して、原秘密鍵Ks0の配布を、データ管理センタに要求する。なお、原著作が、情報提供者あるいはデータベースに原データコンテンツを譲渡あるいは管理預託しておき、情報提供者あるいはデータベースが原著作の役割を果たすようにすることもできる。また、原著作Aが原秘密鍵Ks0を保管し、データ管理センタに依存することなく原データコンテンツM0の暗号化を行うことも可能であるが、ユーザ（データ利用者）による原データコンテンツM0の利用を行うためにはデータ管理センタに原秘密鍵Ks0が保管されている必要がある。

【0061】(2) 原秘密鍵Ks0の配布を要求されたデータ管理センタは、著作権ラベルLc0とともに著作権ラベルLc0に対応させた原秘密鍵Ks0を原著作Aの公開鍵Kb0を用いて暗号化し、

$Cks0kb0 = E(Ks0, Kb0)$

暗号化原秘密鍵Cks0kb0を、原著作Aに送付する。

【0062】データ管理センタは、このときに著作権ラベルLc0をMD5等のアルゴリズムを用いて一方向ハッシュ、例えば16バイトのデータ量に、を行い著作権ラベル指紋F0を作成し、原著作Aに送付する。この、電子指紋は原データコンテンツあるいは加工が行われ加工データコンテンツが得られる度に各々の加工データコンテンツについて作成され、データコンテンツとともに転送される。

【0063】(3) 暗号化原秘密鍵Cks0kb0を配付された原著作Aは、暗号化原秘密鍵Cks0kb0を原著作Aの専用鍵Kv0を用いて復号し、

$Ks0 = D(Cks0kb0, Kv0)$

復号された原秘密鍵Ks0を用いて原著作物データコンテンツM0を暗号化し、

$Cm0ks0 = E(M0, Ks0)$

暗号化原データコンテンツCm0ks0と著作権ラベルLc0及び著作権ラベル指紋F0を、第1ユーザU1に転送する。

【0064】(4) 暗号化原著作物データコンテンツCm0ks0と著作権ラベルLc0及び著作権ラベル指紋F0を転送された第1ユーザU1は、著作権ラベルLc0と著作権ラベル指紋F0及び第1ユーザラベルLu1を提示して、原秘密鍵Ks0の配布を、データ管理センタに要求する。

【0065】(5) 原秘密鍵Ks0の配布を要求されたデータ管理センタは、提示された著作権ラベルL0の正当性を著作権ラベル指紋F0によって確認して、第1ユーザラベルLu1を登録するとともに、著作権ラベルLc0に対応する原秘密鍵Ks0を第1ユーザU1の公開鍵Kb1を用いて暗号化して、

$Cks0kb1 = E(Ks0, Kb1)$

暗号化原秘密鍵Cks0kb1を、第1ユーザU1に配布する。

【0066】(6) 暗号化原秘密鍵Cks0kb1を配布された第1ユーザU1は、暗号化原秘密鍵Cks0kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

$Ks0 = D(Cks0kb1, Kv1)$

復号された原秘密鍵Ks0を用いて暗号化原データコンテンツCm0ks0を復号し、

$M0 = D(Cm0ks0, Ks0)$

復号された原データコンテンツM0を加工ツールを用いて加工し、加工データコンテンツMe1を得る。

【0067】このようにして得られた加工データコンテンツMe1にはデータの加工を行った第1ユーザの著作権とともに、原データコンテンツを作成した原著作の著作権も存在している。原データコンテンツM0に関する原著作の著作権は登録された著作権ラベルLc0及び著作権ラベル指紋F0と著作権ラベルLc0に対応させた原秘密鍵Ks0、第1ユーザラベルLu1と第1ユーザラベルLu1に対応させた第1秘密鍵Ks1によって保護す

ることができるが、加工データコンテンツMe1を暗号化する鍵は用意されていないため、加工データコンテンツMe1に関する第1ユーザの二次著作権は未だ保護される状態にはなっていない。

【0068】(7) 加工データコンテンツMe1に関する第1ユーザの二次著作権を保護するために、この実施例においては、加工データコンテンツの著作者である第1ユーザラベルとその電子指紋を利用する。前に説明したように加工著作物は、利用した原データコンテンツ、使用した加工ツールの情報及び加工内容データとによって表現することができるから、第1ユーザラベルいいかえれば第1加工ラベルLe1にはこれらの情報及びデータが記入される。さらに、以後の流通過程における二次著作権保護のために、ユーザU1は第1加工ラベルLe1を、データ管理センタに提示し、このことによってユーザU1の二次著作権の登録が行われる。

【0069】(8) 第1加工ラベルLe1を提示されたデータ管理センタは、提示された原著作権ラベルLc0の正当性を原著作権ラベル指紋F0によって確認して、第1加工ラベルLe1を登録するとともに、第1加工ラベルLe1の電子指紋F1を作成し、第1加工ラベルLe1に対応させた第1加工秘密鍵Kse1をデータ管理センタの第1ユーザU1の公開鍵Kb1で暗号化し、

$Ckse1kb1 = E(Kse1, Kb1)$

暗号化第1加工秘密鍵Ckse1kb1を第1加工ラベルLe1の電子指紋Fe1とともに、第1ユーザU1に送付する。

【0070】(9) 暗号化第1加工秘密鍵Ckse1kb1及び第1加工著作権ラベルLe1の電子指紋Fe1を配布された第1ユーザU1は、暗号化第1加工秘密鍵Ckse1kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

$Kse1 = D(Ckse1kb1, Kv1)$

復号された第1加工秘密鍵Kse1を用いて第1加工データコンテンツMe1を暗号化し、

$Cme1kse1 = E(Me1, Kse1)$

暗号化第1加工データコンテンツCme1kse1を第1加工著作権ラベルLe1及び第1加工著作権ラベルLe1の電子指紋Fe1とともに、第2ユーザU2に転送する。以後、同様な動作が繰り返される。

【0071】なお、各ユーザが、データ管理センタに提示するそのユーザのラベルにそのラベルの一方方向性ハッシュ値をユーザの専用鍵を用いて暗号化したデジタル署名を付け、データ管理センタがそのユーザの公開鍵を用いて暗号化一方方向性ハッシュ値を復号し、そのラベルの一方方向性ハッシュ値を計算し、両一方方向性ハッシュ値を比較することにより、各ユーザラベルの正当性の検証を行うことができる。

【0072】この実施例において、加工データの転送時に暗号化第1加工データコンテンツCme1kse1とともに転送されるのは第1加工著作権ラベルLe1及び第1加工著作権ラベルLe1の電子指紋Fe1だけであるが、他のラ

ベル及び電子指紋も同時に転送されるように構成することもできる。図2に示されたような複数のデータコンテンツを利用して行う加工はデータコンテンツの数が多い分動作が煩雑であるが、単一データコンテンツを利用した加工の場合と同様にして行われるため、説明が冗長にならないように省略する。

【0073】以上説明したシステムでは、データコンテンツは秘密鍵を用いて暗号化されており、その復号用秘密鍵及び保存・複写・転送に用いる再暗号化用秘密鍵はユーザが提示したユーザラベルに基づいてデータ管理センタにより配布される。

【0074】[実施例4] ライセンスネットワークシステムに代表される分散オブジェクトシステムの場合には、大容量のデータ保存装置を有する従来のコンピュータではなく、データ保存装置を有せずデータの入出力及びデータの処理のみを行うネットワークコンピュータの使用が考慮されている。さらには、データ処理機能すら有せずデータの入出力機能のみを有する、大型コンピュータのターミナル装置的なネットワークコンピュータを使用することも考慮されている。このようなネットワークコンピュータはデータ保存装置を有していないため著作物データを保存あるいは複写することはできない。

【0075】次に、このような分散オブジェクトシステムで使用されるデータ保存装置を有していないネットワークコンピュータに対しても適用可能な実施例を説明するが、この実施例は通常のデータ保存装置を有するコンピュータに対しても適用可能であることは当然のことである。

【0076】データ著作権を保護するには著作物の無許可利用を制限するために、何らかの暗号技術を使用する必要がある。実施例3では通常のデータ保存装置を有するコンピュータを対象としたシステムでの著作権を保護するために、暗号化されたデータコンテンツと、データコンテンツを利用するための手がかりとして暗号化されていないラベルを用いている。これに対して、ターミナル装置的な機能しか有していないネットワークコンピュータを対象としたシステムにおいては、データコンテンツが保存、複写あるいは転送されることはないためデータコンテンツを暗号化する必要はない。

【0077】データコンテンツの加工は、原データコンテンツを加工ツールを用いて改変することによって行われ、加工によって得られた加工データコンテンツは、利用した原データコンテンツ、使用した加工ツールの情報及び加工シナリオによって表現することができる。このことは分散オブジェクトシステムについても同様であり、分散オブジェクトシステム上に存在するデータベースのデータコンテンツを利用して加工データコンテンツを作成した場合にも、利用したデータベース、利用した原データコンテンツ、使用した加工ツールの情報及び加工シナリオを特定することによって加工データコンテ

ツを再現することができ、このことは単一のデータベースあるいは複数のデータベースから入手した複数のデータコンテンツを利用した場合であっても同様である。

【0078】図5により実施例4を説明する。この実施例において、データコンテンツを保有している著作権者及び情報提供者（IP）はデータコンテンツを保有していないユーザと区別されてデータ管理センタ等とともにネットワーク側に配置される。この実施例のシステムにおいては公開鍵及び専用鍵が使用される。なお、原データコンテンツがユーザに転送されるときには、安全のために原データコンテンツは秘密鍵をあるいは転送先の公開鍵を用いて暗号化される。

【0079】第1ユーザU1はネットワーク、放送あるいは記録媒体を利用して、データコンテンツの探索を行い必要なデータコンテンツを収集するが、収集された著作物データはユーザU1のメモリ上に1時的に保存されるに止まり、ハードディスクドライブ（HDD）等のデータ保存装置がユーザU1の装置に含まれている場合でもデータコンテンツがデータ保存装置に保存されることはない。データコンテンツが保存されることがないようにするために、保存が行われようとした場合に、メモリ上の著作物データの破壊、メモリ上のデータヘッダの変更、データコンテンツの一方方向ハッシュ値化、ファイル名の保存不能ファイル名への変更等が行われることによりデータコンテンツの保存禁止が行われる。保存禁止は、オブジェクト構造を有するデータコンテンツのプログラム部分に内蔵されたデータ保存禁止プログラムによって行うこともできるが、システム全体あるいはユーザの装置に関わるオペレーティングシステム（OS）によって行われることにより高度の信頼性が得られる。

【0080】複数のデータコンテンツを利用する場合について説明する。

(1)、(2) 第1ユーザU1は第1ユーザラベルLu1を、データ管理センタに提示して、システム内の情報提供者IPのデータライブラリから原データM0i（i=1,2,3...）を収集し、加工ツールPeを入手するが、このとき原データコンテンツM0i及び加工ツールPeは第1ユーザU1の公開鍵Kb1を用いて暗号化されて、

$$Cm0ikb1 = E(M0i, Kb1)$$

$$Cpekb1 = E(Pe, Kb1)$$

暗号化原データコンテンツCm0ikb1及び暗号化加工ツールCpekb1が、第1ユーザU1に配付される。なお、このとき第1ユーザラベルLu1が参照されることにより、原データコンテンツM0i及び加工ツールPeの利用状況もデータ管理センタに記録され、課金に利用される。

【0081】(3) 暗号化原データコンテンツCm0ikb1及び暗号化加工ツールCpekb1を配布された第1ユーザU1は、配布された暗号化原データコンテンツCm0ikb1及び暗号化加工ツールCpekb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

$$M0i = D(Cm0ikb1, Kv1)$$

$$Pe = D(Cpekb1, Kv1)$$

し、復号された加工ツールPeを使用して復号された原データコンテンツM0iを加工し、第1加工データコンテンツM1i（i=1,2,3...）を得る。

【0082】(4) 第1加工データコンテンツM1iを得た第1ユーザU1は、第1加工著作物データコンテンツM1iについての加工データである第1シナリオS1iをデータ管理センタの公開鍵Kbcで暗号化し、

$$Cs1ikbc = E(S1i, Kbc)$$

暗号化第1シナリオCs1ikbcを第1ユーザラベルLu1とともに、データ管理センタに提示し、このことによってユーザU1の二次著作権の登録が行われる。

【0083】(5) 暗号化第1シナリオCs1ikbcを提示されたデータ管理センタは、暗号化第1シナリオCs1ikbcをデータ管理センタの専用鍵Kvcを用いて復号し、

$$S1i = D(Cs1ikbc, Kvc)$$

提示された第1ユーザU1のユーザラベルと復号された第1シナリオS1iに基づき第1加工ラベルLe1を作成し、データ管理センタ内に保管し、第1加工ラベルLe1を第1ユーザU1の公開鍵Kb1を用いて暗号化し、

$$Cle1kb1 = E(Le1, Kb1)$$

暗号化第1加工ラベルCle1kb1を、第1ユーザU1に転送する。

【0084】(6) 暗号化第1加工ラベルCle1kb1を転送された第1ユーザU1は、暗号化第1加工ラベルCle1kb1を第1ユーザU1の専用鍵Kv1を用いて復号し、

$$Le1 = D(Cle1kb1, Kv1)$$

復号された第1加工ラベルLe1を第2ユーザU2の公開鍵Kb2を用いて暗号化し、

$$Cle1kb2 = E(Le1, Kb2)$$

暗号化第1加工ラベルCle1kb2を、第2ユーザU2に転送するが、第1加工著作物データコンテンツM1iあるいは暗号化第1加工著作物データが第2ユーザU2に転送されることはない。

【0085】第1ユーザU1のコンピュータがデータ保存装置を有しているときには収集データコンテンツあるいは加工データコンテンツがデータ保存装置に保存される可能性があるが、保存・複写及び転送を阻止するために、上述の保存禁止が行われる。なお、この場合暗号化第1加工ラベルCle1kb2の代わりに、第1加工ラベルを一方方向ハッシュ値化した電子指紋F1を使用することもでき、このようにすることにより電話音声による簡略化された加工ラベルの転送が可能になる。

【0086】(7) 暗号化第1加工ラベルCle1kb2を転送された第2ユーザU2は、転送された暗号化第1加工ラベルCle1kb2を第2ユーザU2の専用鍵Kv2を用いて復号し、

$$Le1 = D(Cle1kb2, Kv2)$$

第1加工ラベルLe1を第2ユーザU2の専用鍵Kv2を用

いて暗号化し、

$$C1e1kv2 = E (L e1, K v2)$$

暗号化第 1 加工ラベル $C1e1kv2$ を第 2 ユーザラベル $L u2$ とともに、データ管理センタに提示する。

【0087】(8) 暗号化第 1 加工ラベル $C1e1kv2$ と第 2 ユーザラベル $L u2$ を提示されたデータ管理センタは、提示された暗号化第 1 加工ラベル $C1e1kv2$ を第 2 ユーザ $U2$ の公開鍵 $K b2$ を用いて復号し、

$$L e1 = D (C1e1kv2, K b2)$$

復号された第 1 加工ラベル $L e1$ に記載された原データコンテンツ $M0i$ を収集し、原データ $M0i$ を加工ツール $P e$ を用いて同じく第 1 加工ラベル $L e1$ に記載された第 1 シナリオ $S1i$ に基づいて加工して第 1 加工データコンテンツ $M1i$ を再生する。

【0088】第 1 加工データコンテンツ $M1i$ を再生したデータ管理センタは、第 1 加工データコンテンツ $M1i$ 及び加工ツール $P e$ を第 2 ユーザ $U2$ の公開鍵 $K b2$ を用いて暗号化し、

$$C m1ikb2 = E (M1i, K b2)$$

$$C pek2 = E (P e, K b2)$$

暗号化第 1 加工データコンテンツ $C m1ikb2$ 及び暗号化加工ツール $C pek2$ を、第 2 ユーザ $U2$ に転送する。

【0089】(9) 暗号化第 1 加工データコンテンツ $C m1ikb2$ 及び暗号化加工ツール $C pek2$ を配布された第 2 ユーザ $U2$ は、配布された暗号化第 1 データコンテンツ $C m1ikb2$ 及び暗号化加工ツール $C pek2$ を第 2 ユーザ $U2$ の専用鍵 $K v2$ を用いて復号し、

$$M1i = D (C m1ikb2, K v2)$$

$$P e = D (C pek2, K v2)$$

し、復号された加工ツール $P e$ を使用して復号された第 1 加工データコンテンツ $M1i$ を加工し、第 2 加工データコンテンツ $M2i$ ($i=1, 2, 3, \dots$) を得る。

【0090】(10) 第 2 加工著作物データコンテンツ $M2i$ を得た第 2 ユーザ $U2$ は、第 2 加工データコンテンツ $M2i$ についての加工データである第 2 シナリオ $S2i$ をデータ管理センタの公開鍵 $K bc$ で暗号化し、

$$C s2ikbc = E (S2i, K bc)$$

暗号化第 2 シナリオ $C s2ikbc$ を第 2 ユーザラベル $L u2$ とともに、データ管理センタに提示する。

【0091】(11) 暗号化第 2 シナリオ $C s2ikbc$ を提示されたデータ管理センタは、暗号化第 2 シナリオ $C s2ikbc$ をデータ管理センタの専用鍵 $K vc$ を用いて復号し、

$$S2i = D (C s2ikbc, K vc)$$

提示された第 2 ユーザ $U2$ のユーザラベルと復号された第 2 シナリオ $S2i$ に基づき第 2 加工ラベル $L e2$ を作成し、データ管理センタ内に保管し、第 2 加工ラベル $L e2$ を第 1 ユーザ $U2$ の公開鍵 $K b2$ を用いて暗号化し、

$$C1e2kb2 = E (L e2, K b2)$$

暗号化第 2 加工ラベル $C1e2kb2$ を、第 2 ユーザ $U2$ に転送する。

【0092】(12) 暗号化第 2 加工ラベル $C1e2kb2$ を転送された第 2 ユーザ $U2$ は、暗号化第 2 加工ラベル $C1e2kb2$ を第 2 ユーザ $U2$ の専用鍵 $K v2$ を用いて復号し、

$$L e2 = D (C1e2kb2, K v2)$$

復号された第 2 加工ラベル $L e2$ を第 3 ユーザ $U3$ の公開鍵 $K b3$ を用いて暗号化し、

$$C1e2kb3 = E (L e2, K b3)$$

暗号化第 2 加工ラベル $C1e2kb3$ を、第 3 ユーザ $U3$ に転送する。以後、同様な動作が繰り返される。

【0093】この分散オブジェクトシステムを利用する実施例 4 では、データコンテンツはユーザが保存せず、データベースにのみ保存されている、一方ユーザはユーザの情報及び加工に関する情報すなわち、利用した原データコンテンツ、使用した加工ツールの情報及び加工シナリオ及び加工したユーザ情報が記載された加工ラベルのみを管理保存し、この加工ラベルのみが暗号化されてユーザ間で転送される。したがって、著作物データコンテンツが保存・複写あるいは転送されることはない。

【0094】なお、再暗号用の鍵が復号用の鍵と同時に配布されるシステムと、再暗号用の鍵が復号用の鍵と別々に配布されるシステムとを一つのシステム中に共存させ、適宜選択して利用するように構成することも可能である。

【0095】〔実施例 5〕原データコンテンツ及び加工データコンテンツを流通させるデータコンテンツ流通システムの実施例を図 6 により説明する。このシステムにおいて取り扱われる原データコンテンツはオブジェクトであり、加工データコンテンツは原データコンテンツオブジェクトを加工シナリオによってリンクさせたものとして表現される。したがって、流通するのは加工シナリオのみであり、加工シナリオを入手したユーザは加工シナリオに従って使用されている原データコンテンツを収集しリンクさせて加工データコンテンツを再現させる。この場合、原データコンテンツの収集及びリンク作業はユーザ自身が行ってもよいが、システム側で行うかあるいはエージェントプログラムに行わせれば負担が軽減される。

【0096】このシステムの中核をなすデータコンテンツ流通センタは、ネットワーク上に存在するデータコンテンツデータベース、加工シナリオデータベース、鍵管理センタ、データコンテンツ流通管理センタから構成されている。データコンテンツデータベースは、情報提供者 (IP) が供給した原データコンテンツを保存し、ユーザの要求に対応して供給する。シナリオデータベースは、ユーザが原データコンテンツあるいはユーザが創作したユーザデータコンテンツを利用して加工データコンテンツを得た場合の加工シナリオを保存し、ユーザの要求に対応して供給する。鍵管理センタは、原データコンテンツ、ユーザデータコンテンツ及び加工シナリオの暗号／復号用秘密鍵を保存し、ユーザの要求に対応して供

給する。データコンテンツ流通管理センタは、原データコンテンツあるいは加工データコンテンツをカタログ化して広告し、ユーザへの販売管理及び課金を行うとともにデータコンテンツデータベースに保存されるデータコンテンツの著作権ラベルの管理を行う。加工シナリオ流通管理センタは、加工データコンテンツをカタログ化して広告し、ユーザへの販売管理及び課金を行う。さらに、必要に応じて加工シナリオに基づいて原データコンテンツの収集及びリンク作業を行うとともに加工シナリオデータベースに保存される加工シナリオの加工ラベルの管理を行う。これらデータコンテンツ流通センタを構成する各要素の具体的な動作については、これまでに説明した内容と重複するため、ここでは説明を省略する。

【0097】(1) 情報提供者 $I P_i$ ($i=1, 2, 3, \dots$ 、以降同様) は、原データコンテンツ $M0i$ を原秘密鍵 $Ks0i$ を用いて暗号化し、

$$Cm0iks0i = E(M0i, Ks0i)$$

対応する原秘密鍵 $Ks0i$ をデータコンテンツ流通センタの公開鍵 Kbc を用いて暗号化し、

$$Cks0ikbc = E(Ks0i, Kbc)$$

暗号化原データコンテンツ $Cm0iks0i$ (図では“ $m0i$ ”と表示) 及び暗号化原秘密鍵 $Cks0ikbc$ (図では“ $ks0i$ ”と表示) をデータコンテンツ流通センタに供給する。

【0098】原秘密鍵 $Ks0i$ は情報提供者 $I P_i$ が用意してもあるいは情報提供者 $I P_i$ が鍵管理センタに生成を依頼してもよい。原秘密鍵 $Ks0i$ を鍵管理センタが生成する場合には生成された原秘密鍵 $Ks0i$ は情報提供者 $I P_i$ の公開鍵 $Kb0i$ を用いて暗号化されて、

$$Cks0ikb0i = E(Ks0i, Kb0i)$$

暗号化原秘密鍵 $Cks0ikb0i$ が情報提供者 $I P_i$ に配送され、情報提供者 $I P_i$ は専用鍵 $Kv0i$ を用いて復号し、

$$Ks0i = D(Cks0ikb0i, Kv0i)$$

復号された原秘密鍵 $Ks0i$ を原データコンテンツ $M0i$ の暗号化に用いる。

【0099】データコンテンツ流通センタは、供給された暗号化原秘密鍵 $Cks0ikbc$ をデータコンテンツ流通センタの専用鍵 Kvc を用いて復号化し、

$$Ks0i = D(Cks0ikbc, Kvc)$$

復号された原秘密鍵 $Ks0i$ を用いて暗号化原データコンテンツ $Cm0iks0i$ を復号し、

$$M0i = D(Cm0iks0i, Ks0i)$$

復号された原データコンテンツ $M0i$ 及びこれに対応する原秘密鍵 $Ks0i$ をデータコンテンツデータベースに保存する。なお、情報提供者あるいはデータコンテンツ流通センタが原データコンテンツ $M0i$ に不正利用確認のための透かしを付与して保存することもできる。

【0100】コンテンツ流通管理センタは原データコンテンツの利用促進のため、原データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化してデータコンテンツ

流通センタ内に掲示する。

【0101】(2) カタログ化された原データコンテンツを閲覧した第1ユーザ $U1i$ は、第1ユーザラベル $Lu1i$ 及び第1ユーザ $U1i$ の公開鍵 $Kb1i$ を提示し、利用を希望する原データコンテンツを指定してデータコンテンツ流通センタに利用申込みを行う。

【0102】(3) 原データコンテンツ $M0i$ の利用申込みを受けたデータコンテンツ流通センタは、課金及び身元確認のためユーザラベル $Lu1i$ を確認し、原データコンテンツ $M0i$ に対応する原秘密鍵 $Ks0i$ を用いて暗号化し、

$$Cm0iks0i = E(M0i, Ks0i)$$

原秘密鍵 $Ks0i$ を第1ユーザ $U1i$ の公開鍵 $Kb1i$ を用いて暗号化し、

$$Cks0ikb1i = E(Ks0i, Kb1i)$$

暗号化原データコンテンツ $Cm0iks0i$ 及び暗号化原秘密鍵 $Cks0ikb1i$ (図では“ $ks0i$ ”と表示) を第1ユーザ $U1i$ に配送するとともに、原データコンテンツの使用について第1ユーザ $U1i$ に対する課金を行う。

【0103】(4) 暗号化原データコンテンツ $Cm0iks0i$ 及び暗号化原秘密鍵 $Cks0ikb1i$ を配送された第1ユーザ $U1i$ は、暗号化原秘密鍵 $Cks0ikb1i$ を第1ユーザ $U1i$ の専用鍵 $Kv1i$ を用いて復号し、

$$Ks0i = D(Cks0ikb1i, Kv1i)$$

次に復号された原秘密鍵 $Ks0i$ を用いて暗号化原データコンテンツ $Cm0iks0i$ を復号し、

$$M0i = D(Cm0iks0i, Ks0i)$$

復号された原データコンテンツ $M0i$ を利用して新規な第1加工データコンテンツ $M1i$ を作成する。

【0104】前に述べたように、データコンテンツの加工には単一の原データコンテンツを利用する場合と、複数の原データコンテンツを利用する場合があり、これらにはさらにユーザのデータコンテンツが加えられる場合がある。したがって、この実施例において加工に利用されるデータコンテンツには単一のデータコンテンツの他に、複数の原データコンテンツ、ユーザのデータコンテンツがあり、これらのデータコンテンツと加工内容である加工シナリオによって加工データコンテンツは構成され、すなわちこれらを手することにより加工データコンテンツを再現することができる。

【0105】ところで、原データコンテンツは本来データコンテンツ流通センタのデータコンテンツデータベースに保存されているものであるから、データコンテンツの加工によって新規に生成されたことによりデータコンテンツ流通センタに未だ保存されていないデータはユーザのデータコンテンツと加工シナリオである。したがって、これらをデータコンテンツ流通センタに保存することによりデータコンテンツの加工を行ったユーザの第1ユーザデータコンテンツを原データコンテンツと同様に取り扱うことが可能になり、そのユーザも情報提供者と

なることが可能になる。

【0106】(5) 第1加工データコンテンツM1iは、原データコンテンツM0iと第1加工シナリオS1iから構成され、さらに場合によっては構成要素として第1ユーザデータコンテンツMu1iが加えられる。これらの要素中、原データコンテンツM0iはデータコンテンツ流通センタのデータコンテンツデータベースに保存されているから、新規にデータコンテンツ流通センタに保存する必要があるのは第1加工シナリオS1iと第1ユーザデータコンテンツMu1iである。

【0107】そのために第1ユーザU1iは第1秘密鍵Ks1iを用意し、第1加工シナリオS1iと第1ユーザデータコンテンツMu1iを第1秘密鍵Ks1iを用いて暗号化し、

$$Cs1iks1i = E(S1i, Ks1i)$$

$$Cmu1iks1i = E(Mu1i, Ks1i)$$

第1秘密鍵Ks1iをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化し、

$$Cks1ikbc = E(Ks1i, Kbc)$$

暗号化第1加工シナリオCs1iks1i (図では、“s1i”と表示)、暗号化第1ユーザデータコンテンツCmu1iks1i (図では、“m1i”と表示)及び暗号化第1秘密鍵Cks1ikbc (図では、“ks1i”と表示)をデータコンテンツ流通センタに転送する。

【0108】第1秘密鍵Ks1iは第1ユーザU1iが用意してもあるいは第1ユーザU1iが鍵管理センタに生成を依頼してもよい。第1秘密鍵Ks1iを鍵管理センタが生成する場合には生成された第1秘密鍵Ks1iは第1ユーザU1iの公開鍵Kb1iを用いて暗号化されて、

$$Cks1ikb1i = E(Ks1i, Kb1i)$$

暗号化第1秘密鍵Ck1ikb1iが第1ユーザU1iに配送され、第1ユーザU1iは専用鍵Kv1iを用いて復号し、

$$Ks1i = D(Cks1ikb1i, Kv1i)$$

復号された第1秘密鍵K1iを第1加工シナリオS1i及び第1ユーザデータコンテンツMu1iの暗号化に用いる。

【0109】データコンテンツ流通センタは、データコンテンツ流通センタの専用鍵Kvcを用いて転送された暗号化第1秘密鍵Cks1ikbcを復号し、

$$Ks1i = D(Cks1ikbc, Kvc)$$

復号された第1秘密鍵Ks1iを用いて暗号化第1加工シナリオCs1iks1i及び暗号化第1ユーザデータコンテンツCmu1iks1iを復号し、

$$S1i = D(Cs1iks1i, Ks1i)$$

$$Mu1i = D(Cmu1iks1i, Ks1i)$$

第1ユーザラベルに基づいて第1ユーザデータコンテンツラベル及び第1加工シナリオラベルを生成し、復号された第1秘密鍵Ks1i、第1加工シナリオS1i、第1ユーザデータコンテンツMu1i及び第1ユーザデータコンテンツラベル及び第1加工シナリオラベルをデータベースに保存する。なお、第1ユーザあるいはデータコン

テンツ流通センタが原データコンテンツM0iに不正利用確認のための透かしを付与して保存することもできる。第1秘密鍵Ks1i、第1加工シナリオS1i及び第1ユーザデータコンテンツMu1iを保存するデータベースは原データコンテンツM0iが保存されているデータコンテンツデータベースであっても、また別にシナリオデータベースを設けることも可能である。

【0110】コンテンツ流通管理センタは第1加工データコンテンツの利用促進のため、第1加工データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化してデータコンテンツ流通センタ内に掲示する。

【0111】(6) カatalog化された原データコンテンツM0i及び第1加工データコンテンツM1iを閲覧した第2ユーザU2iは、第2ユーザラベルLu2i及び第2ユーザU2iの公開鍵Kb2iを提示し、利用を希望する原データコンテンツM0i及び／又は第1加工データコンテンツM1iを指定してデータコンテンツ流通センタに利用申込みを行う。

【0112】(7) 原データコンテンツM0i及び／又は第1加工データコンテンツM1iの利用申込みを受けたデータコンテンツ流通センタは、課金及び身元確認のためユーザラベルLu2iを確認し、利用申込みが行われた原データコンテンツM0iを対応する原秘密鍵Ks0iを用いて、第1加工シナリオS1i及び第1ユーザデータコンテンツMu1iを第1秘密鍵Ks1iを用いて、原秘密鍵Ks0iを公開鍵Kb2iを用いて、第1秘密鍵Ks1iを公開鍵Kb2iを用いて、各々暗号化し、

$$Cm0iks0i = E(M0i, Ks0i)$$

$$Cs1iks1i = E(S1i, Ks1i)$$

$$Cmu1iks1i = E(Mu1i, Ks1i)$$

$$Cks0ikb2i = E(Ks0i, Kb2i)$$

$$Cks1ikb2i = E(Ks1i, Kb2i)$$

暗号化原データコンテンツCm0iks0i (図では“m0i”と表示)、暗号化第1加工シナリオCs1iks1i (図では“s1i”と表示)、暗号化第1ユーザデータコンテンツCmu1iks1i (図では“mu1i”と表示)、暗号化原秘密鍵Cks0ikb2i及び暗号化第1秘密鍵Cks1ikb2iを第2ユーザU2iに転送するとともに、原データコンテンツM0i及び第1加工シナリオS1iの使用について第2ユーザU2iに対する課金を行う。

【0113】(8) 暗号化原データコンテンツCm0iks0i、暗号化第1加工シナリオCs1iks1i、暗号化第1ユーザデータコンテンツCmu1iks1i、暗号化原秘密鍵Cks0ikb2i及び暗号化第1秘密鍵Cks1ikb2iを転送された第2ユーザU2iは暗号化原秘密鍵Cks0ikb2i及び暗号化第1秘密鍵Cks1ikb2iを第2ユーザU2iの専用鍵Kv2iを用いて復号し、

$$Ks0i = D(Cks0ikb2i, Kv2i)$$

$$Ks1i = D(Cks1ikb2i, Kv2i)$$

次に復号された原秘密鍵 $Ks0i$ を用いて暗号化原データコンテンツ $Cm0iks0i$ を、復号された第1秘密鍵 $Ks1i$ を用いて暗号化第1加工シナリオ $Cs1iks1i$ 及び暗号化第1ユーザデータコンテンツ $Cmu1iks1i$ を復号し、

$M0i = D(Cm0iks0i, Ks0i)$

$S1i = D(Cs1iks1i, Ks1i)$

$Mu1i = D(Cmu1iks1i, Ks1i)$

復号された原データコンテンツ $M0i$ 、第1加工シナリオ $S1i$ 及び第1ユーザデータコンテンツ $Mu1i$ を利用して新規な第2加工データコンテンツ $M2i$ を作成する。

【0114】第2ユーザ $U2i$ は第2秘密鍵 $Ks2i$ を用意し、データコンテンツ流通センタのデータベースに保存されていない新規なデータである第2加工シナリオ $S2i$ と第2ユーザデータコンテンツ $Mu2i$ を第2秘密鍵 $Ks2i$ を用いて暗号化し、

$Cs2iks2i = E(S2i, Ks2i)$

$Cmu2iks2i = E(Mu2i, Ks2i)$

第2秘密鍵 $Ks2i$ をデータコンテンツ流通センタの公開鍵 Kbc を用いて暗号化し、

$Cks2ikbc = E(Ks2i, Kbc)$

暗号化第2加工シナリオ $Cs2iks2i$ (図では“ $s2i$ ”と表示)、暗号化第2ユーザデータコンテンツ $Cmu2iks2i$

(図では“ $mu2i$ ”と表示) 及び暗号化第2秘密鍵 $Cks2ikbc$ (図では“ $k2i$ ”と表示) をデータコンテンツ流通センタに転送する。以後、同様な動作が繰り返される。

【0115】【実施例6】データコンテンツ加工者が加工シナリオの使用権をデータコンテンツ取引市場において競売で販売する実施例を図7により説明する。この実施例において加工シナリオの使用権はシステム上の取引市場において競売され、加工シナリオの使用権を入手した加工シナリオ販売者は加工シナリオをユーザに販売あるいは貸与する。

【0116】このシステムにおいて取り扱われる原データコンテンツはオブジェクトであり、加工データコンテンツは原データコンテンツオブジェクトを加工シナリオによってリンクさせたものとして表現される。したがって、売買されるのは加工シナリオのみであり、加工シナリオを購入あるいは借用したユーザは加工シナリオに従って使用されている原データコンテンツを収集しリンクさせて加工データコンテンツを再現させる。この場合、原データコンテンツの収集はユーザ自身が行ってもよいが、システム側で行うかあるいはエージェントプログラムに行わせれば負担が軽減される。

【0117】このシステムの中核をなすデータコンテンツ流通センタは、ネットワーク上に存在する鍵管理センタ、データコンテンツデータベース、データコンテンツ流通管理センタ、加工シナリオデータベース、加工シナリオ競売管理センタから構成されている。データコンテンツデータベースは、情報提供者が供給した原データコンテンツを保存し、データコンテンツ加工者に供給す

る。加工シナリオデータベースは、データコンテンツ加工者が原データコンテンツあるいはデータコンテンツ加工者が創作した加工者データコンテンツを利用して加工データコンテンツを得た場合の加工シナリオを保存し、競売に参加する加工シナリオ販売者に供給する。鍵管理センタは、原データコンテンツ、加工者データコンテンツ及び加工シナリオの暗号/復号用秘密鍵を保存し、データコンテンツ加工者あるいは加工シナリオ販売者に供給する。データコンテンツ流通管理センタは、原データコンテンツをカタログ化して広告し、データコンテンツ加工者への販売管理を行う。加工シナリオ競売管理センタは、加工データコンテンツをカタログ化して広告し、加工シナリオ競売の管理及び課金を行う。さらに、必要に応じて加工シナリオに基づいて原データコンテンツの収集及びリンク作業を行うとともに加工シナリオデータベースに保存される加工シナリオの加工ラベルの管理を行う。これらデータコンテンツ流通センタを構成する各要素の具体的な動作については、これまでに説明した内容と重複するため、ここでは説明を省略する。

【0118】(1) 情報提供者 IPi ($i=1, 2, 3, \dots$ 、以降同様) は、原データコンテンツ $M0i$ を原秘密鍵 $K0i$ を用いて暗号化し、

$Cm0iks0i = E(M0i, Ks0i)$

対応する原秘密鍵 $Ks0i$ をデータコンテンツ流通センタの組織公開鍵 Kbc を用いて暗号化し、

$Cks0ikbc = E(Ks0i, Kbc)$

暗号化原データコンテンツ $Cm0iks0i$ (図では“ $m0i$ ”と表示) 及び暗号化原秘密鍵 $Cks0ikbc$ (図では“ $ks0i$ ”と表示) をデータコンテンツ流通センタに供給する。

【0119】原秘密鍵 $Ks0i$ は情報提供者 IPi が用意してもあるいは情報提供者 IPi が鍵管理センタに生成を依頼してもよい。原秘密鍵 $Ks0i$ を鍵管理センタが生成する場合には生成された原秘密鍵 $Ks0i$ は情報提供者 IPi の公開鍵 $Kb0i$ を用いて暗号化されて、

$Cks0ikb0i = E(Ks0i, Kb0i)$

暗号化原秘密鍵 $Cks0ikb0i$ が情報提供者 IPi に配送され、情報提供者 IPi は IP 専用鍵 $Kv0i$ を用いて復号し、

$Ks0i = D(Cks0ikb0i, Kb0i)$

復号された原秘密鍵 $Ks0i$ を原データコンテンツ $M0i$ の暗号化に用いる。

【0120】データコンテンツ流通センタは、供給された暗号化原秘密鍵 $Cks0ikbc$ をデータコンテンツ流通センタの専用鍵 Kvc を用いて復号し、

$Ks0i = D(Cks0ikbc, Kvc)$

復号された原秘密鍵 $Ks0i$ を用いて暗号化原データコンテンツ $Cm0iks0i$ を復号し、

$M0i = D(Cm0iks0i, Ks0i)$

復号された原データコンテンツ $M0i$ 及びこれに対応する原秘密鍵 $Ks0i$ をデータコンテンツデータベースに保存

する。なお、情報提供者あるいはデータコンテンツ流通センタが原データコンテンツM0iに不正利用確認のための透かしを付与して保存することもできる。

【0121】コンテンツ流通管理センタは原データコンテンツの加工利用促進のため、原データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化してデータコンテンツ流通センタ内に掲示する。

【0122】(2) カatalog化された原データコンテンツを閲覧したデータコンテンツ加工者Eiは、データコンテンツ加工者ラベルLei及びデータコンテンツ加工者Eiの公開鍵Kbiを提示し、利用を希望する原データコンテンツを指定してデータコンテンツ流通センタに利用申込みを行う。

【0123】(3) 原データコンテンツM0iの利用申込みを受けたデータコンテンツ流通センタは、課金及び身元確認のためユーザラベルLeiを確認し、原データコンテンツM0iに対応する原秘密鍵Ks0iを用いて暗号化し、

原秘密鍵Ks0iをデータコンテンツ加工者Eiの公開鍵K

beiを用いて暗号化し、

暗号化原データコンテンツCm0iks0i及び暗号化原秘密鍵Cks0ikbei(図では"ks0i"と表示)をデータコンテンツ加工者Eiに配送するとともに、原データコンテンツの使用についてデータコンテンツ加工者Ei及び最終ユーザに対する課金を行う。

【0124】(4) 暗号化原データコンテンツCm0iks0i及び暗号化原秘密鍵Cks0ikbeiを配送されたデータコンテンツ加工者Eiは、暗号化原秘密鍵Cks0ikbeiをデータコンテンツ加工者Eiの専用鍵Kveiを用いて復号し、

次に復号された原秘密鍵Ks0iを用いて暗号化原データコンテンツCm0iks0iを復号し、

M0i=D(Cm0iks0i, Ks0i)

復号された原データコンテンツM0iを利用して加工データコンテンツMeiを作成する。

【0125】前に述べたように、データコンテンツの加工には単一の原データコンテンツを利用する場合と、複数の原データコンテンツを利用する場合があり、これらにはさらにデータコンテンツ加工者のデータコンテンツが加えられる場合がある。したがって、この実施例において加工に利用されるデータコンテンツには単一のデータコンテンツの他に、複数の原データコンテンツ、データコンテンツ加工者のデータコンテンツがあり、これらのデータコンテンツと加工内容である加工シナリオによって加工データコンテンツは構成され、すなわちこれらを手に入ることにより加工データコンテンツを再現することができる。

【0126】ところで、原データコンテンツは本来デー

タコンテンツ流通センタのデータコンテンツデータベースに保存されているものであるから、データコンテンツの加工によって新規に生成されたことによりデータコンテンツ流通センタに未だ保存されていないデータはデータコンテンツ加工者の加工者データコンテンツと加工シナリオである。したがって、これらをデータコンテンツ流通センタに保存することによりデータコンテンツの加工を行ったデータコンテンツ加工者の加工者データコンテンツを原データコンテンツと同様に取り扱うことが可能になり、そのデータコンテンツ加工者も情報提供者となることが可能になる。そして、さらには加工シナリオ及び/又は加工者データコンテンツの使用権を市場で競売によって売却することも可能である。なお、加工シナリオ及び加工者データコンテンツの使用権の数は1個の加工データコンテンツについて複数個とすることが可能である。

【0127】(5) 加工データコンテンツMeiは、原データコンテンツM0iと加工シナリオSeiから構成され、さらに場合によっては構成要素として加工者データコンテンツMeiが加えられている。これらの要素中、原データコンテンツM0iはデータコンテンツ流通センタのデータコンテンツデータベースに保存されているから、データコンテンツ加工者の新規にデータコンテンツ流通センタに保存する必要があるのは加工シナリオS1iと加工者データコンテンツMediである。

【0128】加工シナリオS1i及び加工者データコンテンツMediの使用権を売却するために、データコンテンツ加工者Eiは秘密鍵Kseiを用意し、加工シナリオSeiと加工者データコンテンツMediを秘密鍵Kseiを用いて暗号化し、

Cseiksei=E(Sei, Ksei)

Cmediksei=E(Medi, Ksei)

秘密鍵Kseiをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化し、

Ckseikbc=E(Ksei, Kbc)

暗号化加工シナリオCseiksei(図では、"sei"と表示)、暗号化加工者データコンテンツCmediksei(図では"medi"と表示)及び暗号化秘密鍵Ckseikbc(図では、"kseik"と表示)をデータコンテンツ流通センタに転送する。

【0129】秘密鍵Kseiはデータコンテンツ加工者Eiが用意してもあるいはデータコンテンツ加工者Eiが鍵管理センタに生成を依頼してもよい。秘密鍵Kseiを鍵管理センタが生成する場合には生成された秘密鍵Kseiはデータコンテンツ加工者Eiの公開鍵Kbeiを用いて暗号化されて、

Ckseikbei=E(Ksei, Kbei)

暗号化秘密鍵Ckseikbeiがデータコンテンツ加工者Eiに配送され、データコンテンツ加工者Eiは専用鍵Kveiを用いて復号し、

$Ksei = D(Ckseikbei, Kvei)$

復号された秘密鍵 Kei を加工シナリオ Sei 及びデータコンテンツ加工者データコンテンツ $Medi$ の暗号化に用いる。

【0130】データコンテンツ流通センタは、データコンテンツ流通センタの専用鍵 Kvc を用いて転送された暗号化秘密鍵 $Ckseikbc$ を復号し、

$Ksei = D(Ckseikbc, Kvc)$

復号された秘密鍵 $Ksei$ を用いて暗号化加工シナリオ $Cseiksei$ 及び暗号化加工者データコンテンツ $Cmediksei$ を復号し、

$Sei = D(Cseiksei, Ksei)$

$Medi = D(Cmediksei, Ksei)$

復号された秘密鍵 $Ksei$ 、加工シナリオ Sei 及び加工者データコンテンツ $Medi$ に各々データコンテンツ加工者ラベル Lei に基づく著作権ラベルを付けてデータベースに保存する。なお、データコンテンツ加工者あるいはデータコンテンツ流通センタが加工シナリオ Sei 及び加工者データコンテンツ $Medi$ に不正利用確認のための透かしを付与して保存することもできる。秘密鍵 $Ksei$ 、加工シナリオ Sei 及びデータコンテンツ加工者データコンテンツ $Medi$ を保存するデータベースは原データコンテンツ $M0i$ が保存されているデータコンテンツデータベースであっても、また別にシナリオデータベースを設けることも可能である。

【0131】データコンテンツ流通センタ内のシナリオ市場管理センタは加工シナリオ及び加工者データコンテンツの競売を行うために、加工データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化し、販売する使用権の数を示してシナリオ販売管理センタ内に掲示して、競売を行うことを告示する。

【0132】(6) カタログ化された加工データコンテンツ Mei を閲覧した複数の加工シナリオ販売者 Di は、加工シナリオ販売者ラベル Ldi 及び加工シナリオ販売者 Di の公開鍵 $Kbdi$ を提示して加工シナリオ Sei 及びデータコンテンツ加工者データコンテンツ $Medi$ の購入申込みを加工シナリオ市場管理センタに行う。

【0133】(7) 加工シナリオ Sei 及びデータコンテンツ加工者データコンテンツ $Medi$ の購入申込みを受けた加工シナリオ市場管理センタは、課金及び身元確認のため加工シナリオ販売者ラベル Ldi を確認し、ネットワーク上で競売を行い複数の加工シナリオ販売者 Di に加工シナリオ Sei 及びデータコンテンツ加工者データコンテンツ $Medi$ の使用権を売却する。なお、前に述べたように加工シナリオ及び加工者データコンテンツの使用権の数は1個の加工データコンテンツについて複数個とすることが可能である。売却先に決定した加工シナリオ販売者 Di は、加工シナリオ販売者 Di の秘密鍵 $Ksdi$ をデータコンテンツ流通センタの公開鍵 Kbc を用いて暗号化し

て、

$Cksdikbc = E(Ksdi, Kbc)$

暗号化秘密鍵 $Cksdikbc$ (図では、“ $ksdi$ ”と表示) を加工シナリオ市場管理センタに配送する。

【0134】(8) 加工シナリオ市場管理センタは提示された暗号化秘密鍵 $Cksdikbc$ をデータコンテンツ流通センタの専用鍵 Kvc を用いて復号し、

$Ksdi = D(Cksdikbc, Kvc)$

復号された加工シナリオ販売者 Di の秘密鍵 $Ksdi$ を用いて加工シナリオ Sei 及びデータコンテンツ加工者データコンテンツ $Medi$ を暗号化し、

$Cseiksdi = E(Sei, Ksdi)$

$Cmediksdi = E(Medi, Ksdi)$

暗号化加工シナリオ $Cseiksdi$ 及び暗号化データコンテンツ加工者データコンテンツ $Cmediksdi$ を加工シナリオ販売者 Di に送付する。また、著作権ラベルの内容はデータコンテンツ加工者ラベル Lei に基づくものからシナリオ販売者ラベル Ldi に基づくものに変更され、その結果、データコンテンツ加工者の秘密鍵 $Ksei$ は使用不可能となり、代わって加工シナリオ販売者の秘密鍵 $Ksdi$ が使用可能となる。なお、この場合著作権ラベルの内容を変更することなく、新規に加工シナリオ販売者ラベル Ldi に基づくものを追加することもできる。

【0135】暗号化加工シナリオ $Cseiksdi$ を購入した加工シナリオ販売者は以後において、購入した加工シナリオの使用権を行使する。なお、原データコンテンツも加工シナリオと同様に競売によって販売することが可能であるが、原データコンテンツの利用者は複数となることもあり得るため、特定の販売者に売却することは避けたい。以後、必要ならば同様な動作が繰り返される。

【0136】本明細書に示された各実施例のデータコンテンツ流通システムにおいて、ユーザ側装置としてハードディスクドライブ等の保存装置を有しないネットワークコンピュータが使用される場合にはデータコンテンツの無料使用、流出等の不正使用問題は生じにくい。ユーザ側装置としてハードディスクドライブ等の保存装置を有する通常のパーソナルコンピュータ等が使用される場合にはこれらの不正使用問題が生じる可能性が大きい。このような問題に対処するために、本発明者が既に $US08/416037(EP677949A2)$ で提案している著作権管理プログラム及びデータコンテンツの再暗号化を採用することが有効であり、その場合に再暗号化等の処理を行う著作権管理プログラムを他のアプリケーションプログラムに優先させることが可能なりリアルタイムOSあるいはエンベデッドシステムと呼ばれる構成とすることにより、不正使用の問題を適切に回避することができる。

【図面の簡単な説明】

【図1】 データ管理システム実施例の構成図。

【図2】 オブジェクトである複数のデータコンテンツ
を利用しての新しいデータコンテンツを作成する説明
図。

【図3】 データ管理システムの他の実施例の構成図。

【図4】 データコンテンツ流通システムの実施例概要
構成図。

【図5】 データコンテンツ流通システムの他の実施例
の概要構成図。

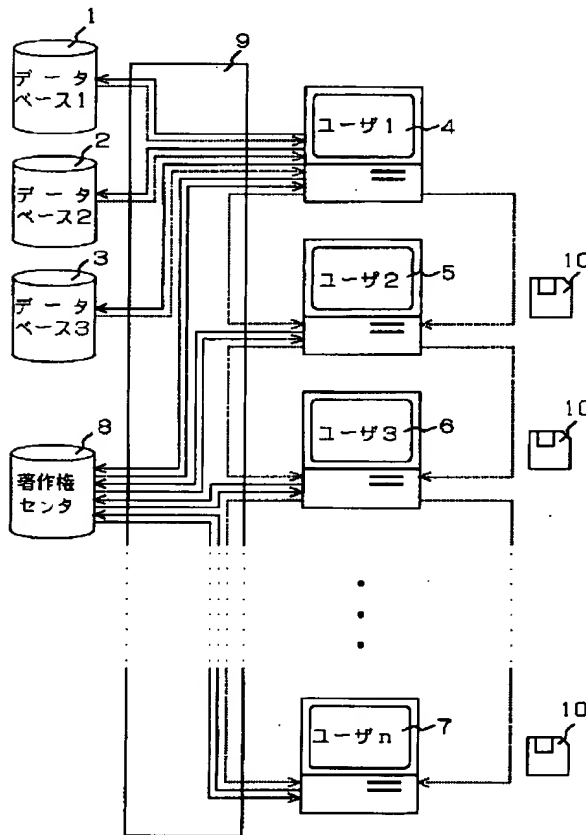
【図6】 データコンテンツ流通システムのさらに他の
実施例の概要構成図。

【図7】 加工シナリオ流通システムの実施例の概要構
成図。

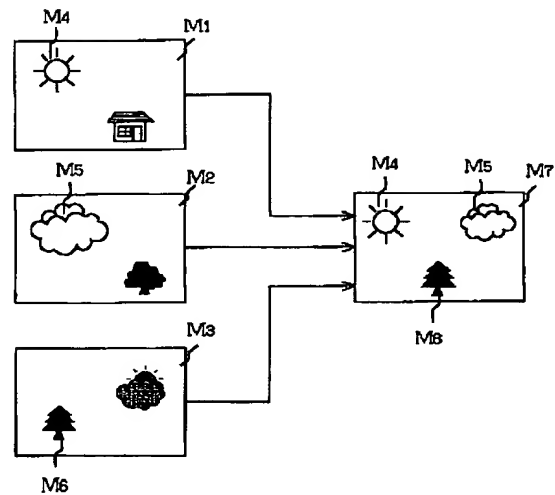
【符号の説明】

- 1, 2, 3, 11 データベース
4, 5, 6, 7, 13, 19 ユーザ端末装置
8 著作権管理センタ
9, 14 通信回線
10, 17, 18 記録媒体
12 鍵管理センタ
15, 16, IP 情報提供者
A 著作権者
10 U1, U2, U3 ユーザ
E データコンテンツ加工者
D 加工シナリオ販売者

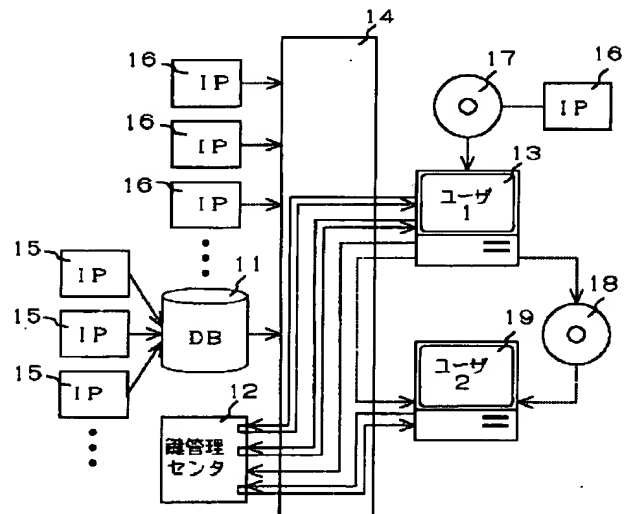
【図1】



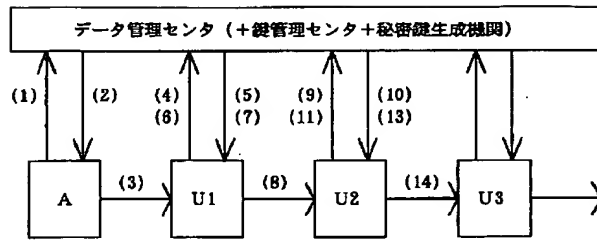
【図2】



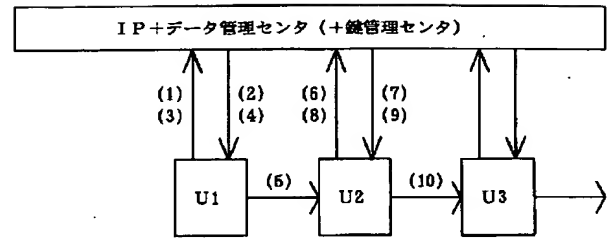
【図3】



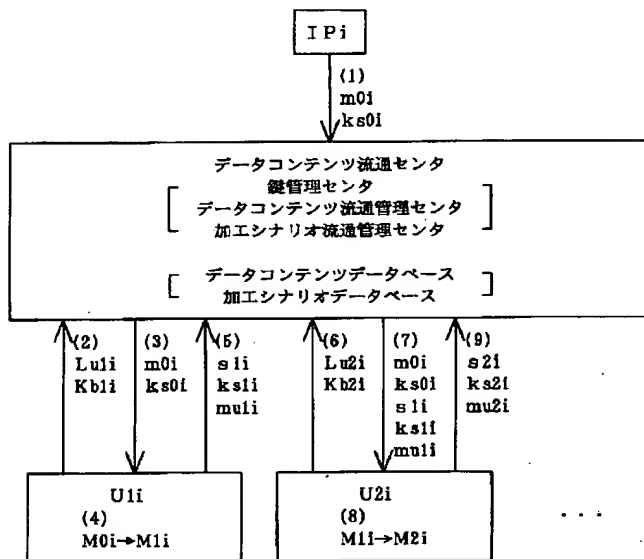
【図4】



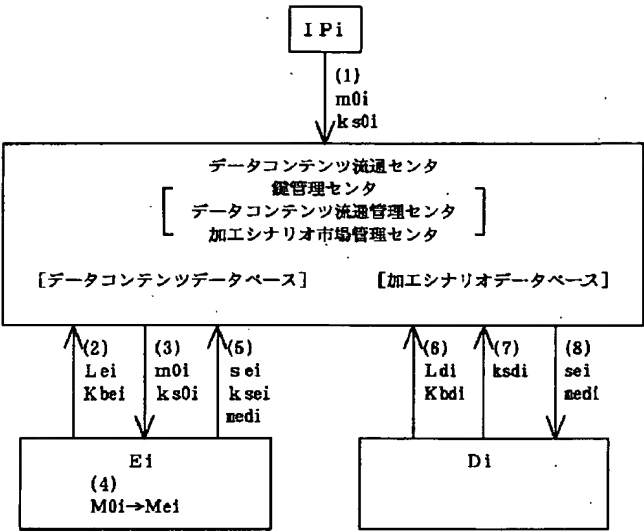
【図5】



【図6】



【図 7】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H O 4 L 9/00

6 0 1 B